

**INTELLIGENT COMMUNICATIONS POINT PLATFORM**

Inventors: Michael Ashdown  
5508 Belle Chasse  
Frisco, Texas 75035  
Citizenship: USA

Hu Shen  
4020 Sunflower Lane  
Plano, Texas 75024  
Citizenship: USA

Steve Lynchard  
14006 Tree Crossing Street  
San Antonio, Texas 78247  
Citizenship: USA

Robert Winslow  
5075 Pear Ridge Drive  
Apartment # 634  
Dallas, Texas 75287  
Citizenship: USA

Assignee: Sevis Systems, Inc.  
17950 Preston Road, Suite 700  
Dallas, Texas 75252

David M. O'Dell, Esq.  
HAYNES AND BOONE, LLP  
901 Main Street, Suite 3100  
Dallas, Texas 75202-3789  
(214) 651-5000  
(214) 200-0853 - Fax  
R-58690\_1.DOC



EXPRESS MAIL NO.: EV 333435992 USDATE OF DEPOSIT: November 14, 2003

This paper and fee are being deposited with the U.S. Postal Service Express Mail Post Office to Addressee service under 37 CFR §1.10 on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Gayle Conner

Name of person mailing paper and fee



Signature of person mailing paper and fee

## INTELLIGENT COMMUNICATIONS POINT PLATFORM

### CROSS-REFERENCE

[0001] This application is a continuation application of U.S. Application No. 09/536,541, filed on March 28, 2000, which is hereby incorporated by reference.

[0002] This application relates to the following co-pending United States Patent Application, incorporates them by reference in their entirety and is assigned to the assignee of the present invention:

Serial No.:	Filing Date:	Inventors:	Title:
09/536,598	03/28/00	Ashdown et al.	New and Improved System and Method for Data Traffic Redirection
09/537,016	03/28/00	Ashdown et al.	System and Method for a Local Number Portability Cache
09/391,295	09/07/99	Ashdown et al.	SS7 Firewall System

### BACKGROUND

[0003] This invention relates generally to the Common Channel Signaling System 7 (SS7) network technology and, more particularly, to a host signaling processing platform that allows multiple SS7 applications to have visibility to SS7 network traffic while also having the ability to control SS7 network traffic.

### BRIEF DESCRIPTION OF THE DRAWINGS

[0004] Figure 1 is a block diagram of signaling end point connections in an SS7 network;



- [0005] Figure 2 is an overview of the ICP Platform;
- [0006] Figure 3 is a block diagram of SS7 network link routing;
- [0007] Figure 4 is a functional diagram of the ICP Platform;
- [0008] Figure 5 is a block diagram of the configuration data flow;
- [0009] Figure 6 is a block diagram of the provisioning data flow; and
- [0010] Figure 7 is a block diagram of the processing data flow.

### **DETAILED DESCRIPTION**

[0011] First a brief overview of one embodiment of the present invention will be described and then will be described in greater detail in reference to the figures. To start with, the ICP Platform is not an end point in the network, but rather an invisible node that sits in front of a Signaling End Point (SEP), which may be, for example, a Signaling Transfer Point (STP), Service Switching Point (SSP), or Service Control Point (SCP). All SS7 links are routed into the ICP and are then routed out to the SS7 network. In addition, the ICP Platform design can be broken down into five parts; SS7 links cards and SS7 stack, interface to the ICM, platform core services, software and hardware control/status, and the application region.

#### **SS7 link cards and SS7 stack**

[0012] The ICP Platform contains multiple T1/E1 link cards. All SS7 links from an SSP are routed into the ICP and then out to the SS7 network. Each link card supports multiple links and processes Message Transfer Part (MTP) layers 1 and 2, while the CPU host card supports the ICP core services, applications, and MTP layer 3. MTP1 defines the physical, electrical, and functional characteristics for the digital signaling link. MTP2 ensures accurate end-to-end transmission of a message across a signaling link. In addition, MTP2 implements flow control, message sequence validation, and error checking. When an error occurs on a signaling link, the message (or set of messages) is retransmitted. Moreover, MTP2, which resides on the link cards, has a failsafe mode. When MTP3 fails, MTP2 will automatically route traffic between the SEP and the SS7 network.



**[0013]** MTP3 provides message routing between signaling points in the SS7 Network and routes traffic away from failed links and signaling points. In addition, MTP3 controls traffic when congestion occurs. In the ICP Platform, two links are used to achieve the usage of one normal link. The ICP sits between an SSP and SS7 network and literally breaks the link into two links. These two links are considered to be one link pair. All SS7 traffic coming in one link will be routed out of the ICP through the other link of the link pair (Figure 3). If the ICP fails due to hardware or software failures, these link pairs close allowing the SS7 traffic to pass through the ICP as if the ICP was not in the network. The link pairs can also be manually closed while still allowing the ICP to have visibility to the SS7 traffic flowing through the link pairs. In addition, link cards route non-SS7 traffic on open DS-0 data lines directly to the other port without going through the ICP.

#### **Interface to the Intelligent Communication Manager (ICM)**

**[0014]** The ICP Platform is managed by the ICM. The ICP interface is the bridge for communications between the ICP and the ICM. Through this interface software, the ICM user can gain access to the ICP core services and application software. The interface allows the user to bring the ICP into service, bring up and down application software, retrieve ICP core service data such as logs and events, retrieve application specific data, and configure/status the ICP hardware/software.

#### **Platform Core Services**

**[0015]** The ICP Platform provides a set of core services for the developers of the applications to use when designing the application, including Logging Data, Process Events, Peg Counting, and the SS7 message interface (Figure 3). Logging Data services allow the applications to collect data which can be passed to the ICM for display to the customer. Process Event service is a method in which alarms can be raised to inform customers of an event that may or may not be critical. Each event is marked with a severity level which indicates to the user whether the event needs attention or not. Peg Counting services are tied in with the traffic metering and measurement (TMM) and bookkeeping processes. Along with the core set of peg counts, applications will also



have their own sets of peg counts that can be collected and displayed on the ICM through the TMM graphical user interface (GUI). The SS7 message interface service allows applications to have access to SS7 traffic flowing through the ICP. The ICP processes all SS7 traffic according to rules. These rules define the actions as to how the SS7 message is going to be processed. Customers can implement rules that will act as a SS7 Firewall to protect the SEP (refer to the pending SS7 Firewall System patent, dated September 7, 1999). Applications can receive SS7 traffic by implementing application rules that pass the message from the stack up through to the application, or can send out SS7 messages through an ICP SS7 API (Application Programming Interface).

#### **Software and Hardware Control/Status**

[0016] Software on the ICP is managed by the platform manager (Figure 4). The platform manager is responsible for starting core services and applications. In the event of a software failure, the platform manager will attempt to restart the failed software along with raising events to the ICM and closing the link pairs so that SS7 traffic is not disrupted. The manager software will send status of the software and overall ICP health to the ICM through the ICP interface software. The hardware and the SS7 stack configuration are handled by System Management Software. Through the use of a configuration file stored on the ICM, the System Management Software programs the hardware interfaces such as the SS7 link cards and configures the SS7 stack software. Status of the hardware and state of the paired links (open or closed) are sent to the ICM through the ICP interface software.



**Application Region**

[0017] The heart of the ICP Platform is its ability to host any number of different SS7 applications (Figure 3). Local Number Portability Cache (LNPC) is just one example of an application that could be developed for the ICP Platform. Through the use of the ICP core services, developers can design applications that can interact with the SS7 network. Application Programming Interfaces (APIs) are available to the application designers. These APIs allow the designers access to the core services and aid in the development process.

[0018] Now referring to the figures, figure 1 represents the end point connections in a SS7 network. Reference numeral 10 designates a signaling end point (SEP) which may be, for example, a Signaling Transfer Point (STP), Service Switching Point (SSP) or Service Control Point (SCP) and reference numeral 12 designates signaling transfer points (STPs). In a typical SS7 network, traffic flows on data links 14 between STPs and SEPs.

[0019] Figure 2 illustrates the placement of the ICP Platform 200 within the SS7 network. The ICP Platform 200 is not an end point in the SS7 network but rather an invisible node that sits in front of an SEP 210/220, which may be for example, an STP, SSP or an SCP. All SS7 data links 14 are routed into the ICP Platform 200 and are then routed out to the SS7 network. The SS7 network includes redundant DS-1 or DS-0A links 14, which are high speed serial links.

[0020] ICP Platform 200 processing distribution is driven by the signaling protocol stack as shown in Figure 2. The MTP1/MPT2 230/240 layer has a number of link cards (E1/T1). The MTP1/MPT2 230/240 layer is loosely coupled with the MTP3 250 layer allowing MTP1/MPT2 230/240 to reside on the link cards and MTP3 250 to reside on the single board computer. MTP1 230 defines the physical, electrical, and functional characteristics for the digital signaling link. MTP2 240, which resides on the link cards, has a failsafe mode. When MTP3 250 fails, MTP2 240 will automatically route traffic back down and out to the SEP. MTP2 240 ensures accurate end-to-end transmission of a message across a signaling link 14. In addition, MTP2 240 implements flow control, message sequence validation, and error checking.



**[0021]** The MTP3 250 layer can interface with multiple MTP2 240 processors on the link cards through a compact Peripheral Component Interconnect (cPCI) bus. By modifying the MTP3 250 layer to disable message discrimination, all messages are allowed to be passed up to the ICP Platform 200 for processing. The MTP3 250 layer can be easily modified by making appropriate changes in the SS7 protocol stack being used.

**[0022]** In addition, MTP3 250 manages the Message Signaling Unit (MSU)/Link association and has end to end management message coordination. MTP3 250 also provides message routing between signaling points 210/220 in the SS7 Network, and can route traffic away from failed links and signaling points. Moreover, MTP3 250 controls traffic when congestion occurs.

**[0023]** The Core Services 260 layer supports various support services and signaling processes to distribute traffic upwards to the Applications 270 layer and accept downward message routing requests. The Core Services 260 layer contains various subsystems and processes within these subsystems that developers of applications can use when designing applications.

**[0024]** The Applications 270 layer contains all the applications that are implemented above the Core Services 260 layer. The Applications 270 layer supports various applications that can monitor, modify, or create messages. Each application can process its own set of messages, use its own rules and can be independent of other applications in general. In addition, one or more of the application processes may be running at a given time to load-share the work.

**[0025]** As shown in Figure 3, a SS7 MTP3 MSU 300 addressed for a signaling point, e.g., 220, travels from a signaling point, e.g., 210, through the ICP Platform 200. The MSU 300 goes through a MTP1 port 230 and then travels up the SS7 protocol stack through the MTP2 240 I/O card and MTP3 250 stack. The MTP3 250 stack may reside on the CPU card, or on the I/O card. A heartbeat signal 310 is maintained between MTP2 240 and MTP3 250. Loss of the heartbeat 310, indicating a failure of the CPU cards in the MTP3 250 layer, results in a failsafe mode (closed mode). During a failsafe mode, message traffic is passed up only to MTP2 240 and is then routed back down and out. If the CPU is available, a copy of the MSU 300 is passed to MTP3 250



for non-intrusive processing. During normal operation (open mode), data is transmitted between MTP1/MTP2 230/240 and MTP3 250. The MSU 300 is then delivered to Core Services 260 which contains various subsystems and processes within these subsystems. Some of those subsystems and processes will be described in detail below.

**[0026]** The Platform Control Subsystem (PCSS) 311 has data provisioning capability and is also responsible for the management of all the other subsystems. In particular it starts and stops all the other processes in a controlled manner. The Signaling Subsystem (SGSS) 312 routes and distributes SS7 messages. This subsystem processes every message that passes through the ICP Platform 200. However, since Fill-in Signal Unit (FISU) messages do not pass up to the ICP platform 200, they are not processed by the SGSS 312. The Interface Subsystem (IFSS) 313 is responsible for the external system interface. In addition, the ICP System has the capability to interface with multiple Intelligent Communications Managers (ICMs) 320, and with other ICP Platforms 200. Moreover, a single ICP Platform 200 may be distributed in multiple processors. The IFSS 313 provides the network interface commonly used for all these conditions.

**[0027]** The Accounting Subsystem (ACSS) 314 is responsible for collecting the Traffic Metering and Measurement (TMM) data and statistic messages from subsystems that generate these messages. The Recording Subsystem (RCSS) 315 is responsible for collecting event and log messages for all other subsystems. Event messages are accumulated over a short period of time while the events are buffered and duplicates are filtered out. The various processes in the Data Management Subsystem (DMSS) 316 provide functions for data storage and retrieval, data synchronization, data distribution, data partition management, etc. Furthermore, the Utility Subsystem (UTSS) 317 contains library routines that are developed for re-use by all subsystem processes.

**[0028]** The Intelligent Communication Manager (ICM) 320, a control and management device, is connected via the TCP/IP link 330 to the ICP Platform 200 for storage and display of logs, alerting, programming control policy rules, providing simple visibility, configuration, and other operational features of the ICP Platform 200. Multiple ICP Platforms 200 can be managed by one ICM 320. Logs are routed via the TCP/IP link 330 from the ICP 200 to the ICM 320 and may range from simple events to



full SS7 call or transaction messages. The TCP/IP link 330 provides communication including, but not limited to, File Transfer Protocol (FTP) Services and Internet Services between the ICP 200 and the ICM 320.

**[0029]** The ICP Platform 200 has the capability to view data traversed on MTP2 data links 14 and signaling units, except the Fill-in Signal Unit (FISU). In addition, the ICP Platform 200 can view all MSUs 300, i.e., network management, traffic routing, test and upper layer protocols on MTP3 250 and can decode all Integrated Service Digital Network (ISDN) User Part (ISUP) messages and view all ISUP parameters and sub-fields. While not shown, it is understood that the ICP Platform 200 is can also communicate within an enterprise network with various hosts for providing management, configuration, and reporting functions.

**[0030]** The ICP Platform 200 is a fully active datalink layer (layer 2 of the seven layer Open Systems Interconnect (OSI) network model) device while providing layer three and above visibility and control. Network layer control messages, such as re-alignment messages, are transferred autonomously from node to node, e.g., from the SEP 210 to the SEP 220, within the SS7 network. The ICP Platform 200 manages these messages and coordinates control between the end nodes 210/220. This allows end nodes to operate as masters of MTP2 240, while communicating directly to the ICP Platform 200. MTP3 MSUs 300 are transferred end-to-end making the ICP Platform 200 appear invisible to each SEP 210/220, at the network layer and above.

**[0031]** The ICP Platform 200 is a full MTP2 signaling link terminal. It also manages MTP3 management messages between nodes 210 and 220. Additionally, it manages coordination of MTP3 traffic management; link management, and route management messages to synchronize MTP2 events between the two links. Functionally, the ICP Platform 200 consists of SS7 I/O logic, which contains MTP1/MTP2 230/240, and MTP3 250 SS7 stacks, located on the I/O card. The function of the stacks process MSUs 300 for MTP3 250. Moreover, the ICP Platform 200 contains MTP3 control logic located on the CPU card. These functions work independently of each other and provide a higher level visibility by processing signaling units into MSUs 300 and MSUs into protocol data units (PDUs) (layer 4 and above of the seven layer OSI network model).



**[0032]** Figure 4 illustrates a functional diagram of the Intelligent Communications Point (ICP) Platform 200. SS7 traffic 400 flows in and out the Signaling Subsystem 312 (SGSS) through the SS7 stack (MTP1/MTP2 230/240 and MTP3 layer 250). SS7 messages are distributed to the processes in the Application Subsystem 270 (APSS). The APSS 270 sends ISUP messages to the SGSS 312 and in some cases the actions that it wants the SGSS 312 to carry out, such as start/stop sending MSU 300, and block an SS7 message. In sum, the ICP Platform 200 combines call state monitoring, line control, and transaction state control for implementing access and service control functions.

**[0033]** The ICP Platform 200 may be implemented with commercially available components as will be understood by those skilled in the art. While not shown, it is understood that the ICP Platform 200 is controlled by computer programming instructions stored in memory within the ICP Platform 200 and potentially other components of the system connected to the ICP Platform 200.

**[0034]** The Platform Control Subsystem (PCSS) 311 is responsible for the management of all other subsystems. PCSS 311 processes, which include the Platform Control Process, the Rule Provisioning Process and the SS7 Provisioning Process, have various responsibilities within the ICP Platform 200. The Platform Control Process is ordinarily the first process to start on the ICP Platform 200 and manages all other processes running on the ICP Platform 200. The Rule Provisioning Process manages the process configuration profile and the application rule repository. This process receives updates from the IFSS 313 and makes updates to the DMSS 316. The SS7 Provisioning Process is responsible for SS7 Node provisioning. This process will receive updates from the IFSS 313 and will make updates to the SS7 stack, using vendor provided programming interfaces.

**[0035]** The Signaling Subsystem (SGSS) 312, which is part of the core services layer 260, contains the ISDN User Part (ISUP) process 410, the Signaling Connection Control Point (SCCP) process 420, the Signaling Network Management 430 (SNM) and the Signaling Network Testing 430 (SNT). All ISUP process 410 and SCCP process 420 traffic can be processed through a SS7 firewall to enforce control policy rules. Management messages such as re-alignment messages are controlled by the ICP



Platform's 200 control message manager application. Some of the common functions provided by the ISUP process 410, SCCP process 420 and SNM/SNT 430 are to generate events to report process start and stop and to report abnormalities. In addition, they inform the MTP3 layer 250 of any status change so that traffic can be started or stopped.

**[0036]** The ISUP process 410 contained in the SGSS 312 is responsible for receiving and forwarding ISUP messages between the MTP3 layer 250 and the Application Layer 270. This process maintains connectivity to the Application Layer 270 process and determines readiness of the ISUP message processing capability, and decodes and encodes the ISUP header. In addition, the ISUP process 410 distributes messages to the Application Layer 270 processes, discards message response if timeout occurs, and takes default action if message response timeout occurs.

**[0037]** The SCCP process 420 is responsible for receiving and forwarding SCCP messages between the MTP3 layer 250 and the Application Layer 270. The SCCP process 420 provides communications between signaling nodes 210 and 220 and provides specialized routing and management functions necessary to support routing to partitioned and/or duplicate databases. In addition, this process returns messages back to MTP3 250 when message is checked OK.

**[0038]** The SNM/SNT process 430 is responsible for receiving and forwarding SNM/SNT, and in particular the Link Status Signal Unit (LSSU) messages and any other messages that the ISUP process 410 and SCCP 420 process can not process. In addition, SNM/SNT process 430 generates Traffic Metering and Measurement (TMM) data and generates events to report LSSU data.

**[0039]** The APSS 270 sends MSUs 300 to the ICM 320 through the Interface Subsystem 313 (IFSS). TMM data is generated by both the APSS 270 and the SGSS 312. Statistics are only generated by the APSS 270 and are sent to the ICM 320 through the Accounting Subsystem 314 (ACSS). Every subsystem generates events and logs that are sent to the ICM 320 through the Recording Subsystem (RCSS) 315.

**[0040]** The ICM 320 provides configuration data for the ICP Platform 200 and the SS7 stack. As illustrated in Figure 5, configuration data is sent to the PCSS 311 through the IFSS 313. The PCSS 311 updates the database with platform configuration



through the DMSS 316. SS7 node configuration is sent to the UTSS 317. UTSS 317 interfaces with the SS7 stack (vendor software portion) to change stack configuration. In addition, the ICM 320 provides rules to the APSS 270 and SGSS 312, which use the rules to determine message distribution and processing. Rules are first passed to the Platform Control Subsystem 311 (PCSS) which updates the database at the Data Management Subsystem 316 (DMSS). As illustrated in Figure 6, rules are first passed from the IFSS 313 to the PCSS 311 which updates the database at the DMSS 316. The APSS 270 and the SGSS 312 then read the rules as needed. The ICM 320 also sends the rule switching command (CMD) to the PCSS 311, which is processed and used in the same way as the rules.

**[0041]** Figure 7 illustrates SS7 traffic 400 distribution and supporting data flow in the system. SS7 traffic 400 flows in and out the SGSS 312. ISUP and MSU messages are distributed to the processes in the APSS 270. The APSS 270 sends ISUP messages to the SGSS 312. The APSS 270 sends MSU data through the IFSS 313. TMM data is generated by both the APSS 270 and the SGSS 312 and is sent to the ICM 320 through the ACSS 314. Statistics are generated by the APSS 270 and are sent to the ICM 320 through the ACSS 314. Every subsystem generates event and log data that are sent to the ICM 320 through the RCSS 315.

**[0042]** It is understood that the present invention can take many forms and embodiments. The embodiments shown herein are intended to illustrate rather than to limit the invention, it being appreciated that variations may be made without departing from the spirit of the scope of the invention. The algorithms and process functions performed by the system may be organized into any number of different modules or computer programs for operation on one or more processors or workstations within the system. Different configurations of computers and processors for the system are contemplated. The programs used to implement the methods and processes of the system may be implemented in any appropriate programming language and run in cooperation with any hardware device. The system may be used for service providers, Internet Service Providers, enterprises, and may other entities utilizing SS7 signaling devices.



**[0043]** Although illustrative embodiments of the invention have been shown and described, a wide range of modification, change and substitution is intended in the foregoing disclosure and in some instances some features of the present invention may be employed without a corresponding use of the other features. Accordingly, it is appropriate that the appended claims be construed broadly and in a manner consistent with the scope of the invention.